(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－215284

(43)公開日　平成10年(1998)８月11日

(51)Int.Cl.[6]	識別記号	ＦＩ		
H04L 12/66		H04L 11/20		B
G06F 15/00	330	G06F 15/00	330	B
G09C 1/00	660	G09C 1/00	660	E
H04L 9/32		H04M 3/00		B
H04M 3/00		H04L 9/00	673	C

審査請求　未請求　請求項の数８　ＯＬ　（全14頁）　最終頁に続く

(21)出願番号　特願平9－15147

(22)出願日　平成９年(1997)１月29日

(71)出願人　597013076
株式会社アド・ホック
北海道札幌市中央区南２条西７丁目６－２　日宝南２条ビル５階

(72)発明者　澤田　原
北海道札幌市中央区南２条西７丁目６－２　日宝南２条ビル５階　株式会社アド・ホック内

(72)発明者　曽田　亮
北海道札幌市中央区南２条西７丁目６－２　日宝南２条ビル５階　株式会社アド・ホック内

(74)代理人　弁理士　木内　光春

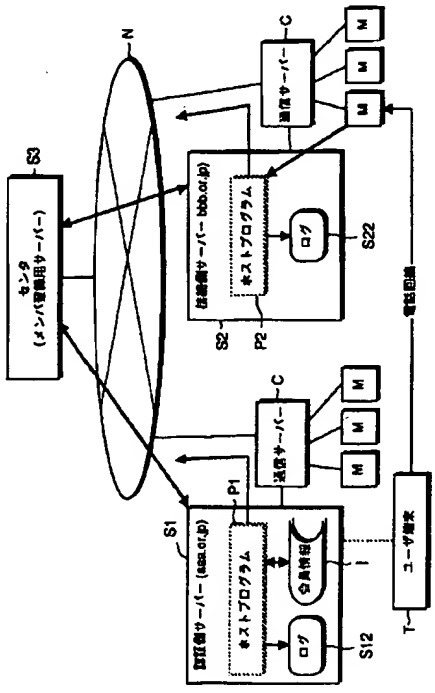
最終頁に続く

(54)【発明の名称】ネットワーク接続システム及びネットワーク接続方法

(57)【要約】

【課題】　複数のサーバー間で会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システムを提供する。

【解決手段】　ユーザーは、自己の会員情報を保有する認証側サーバーＳ１が混雑しているときや地理的に遠い場合、他のサーバーである接続側サーバーＳ２にユーザＩＤとパスワードを送信することによって接続要求を行う。ユーザが送信したユーザＩＤとパスワードは、接続側サーバーＳ２から認証側サーバーＳ１に転送され、認証側サーバーＳ１で会員情報と照合することによってユーザ認証が行われる。接続側サーバーＳ２では、ユーザ認証の結果を受けてログイン処理が行われるので、ユーザはインターネット接続サービスを利用することができる。



1

【特許請求の範囲】

【請求項１】　ネットワークへの接続回線設備を備えた複数のサーバーを有し、

前記サーバーは、

ユーザに関する会員情報を有する認証側サーバーと、

前記認証側サーバーと所定の関係を有する接続側サーバーを含み、

前記接続側サーバーは、ユーザから送信されるユーザＩＤ及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供する接続手段を有し、

前記認証側サーバーは、前記接続側サーバーから送信されるユーザＩＤ及びパスワードを前記会員情報と照合することによってユーザ認証を行うユーザ認証手段を有することを特徴とするネットワーク接続システム。

【請求項２】　前記接続側サーバー及び認証側サーバーはそれぞれ、前記ネットワークへの接続の開始及び終了に関する所定の情報を送受信することによって、接続ログを記録する記録手段を有することを特徴とする請求項１記載のネットワーク接続システム。

【請求項３】　前記接続側サーバーの前記記録手段及び前記認証側サーバーの前記記録手段は、前記接続の開始から終了に至る間、所定の間隔で所定の情報を送受信することによって前記接続が継続しているか否かを確認するように構成されたことを特徴とする請求項２記載のネットワーク接続システム。

【請求項４】　相互に所定の関係を有する複数のサーバーをメンバとして登録する登録手段と、

任意のサーバーがメンバであるか否かの問い合わせに応答するサーバー認証手段と、

を有するメンバ登録用サーバーを備えたことを特徴とする請求項１，２又は３記載のネットワーク接続システム。

【請求項５】　前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーが、

前記ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段を有することを特徴とする請求項１，２，３又は４記載のネットワーク接続システム。

【請求項６】　ネットワークへの接続回線設備を備えた複数のサーバーを用い、

前記サーバーは、

ユーザに関する会員情報を有する認証側サーバーと、

前記認証側サーバーと所定の関係を有する接続側サーバーを含むネットワーク接続システムにおいて、

前記接続側サーバーは、ユーザから送信されるユーザＩＤ及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供し、

前記認証側サーバーは、前記接続側サーバーから送信されるユーザＩＤ及びパスワードを前記会員情報と照合することによってユーザ認証を行うことを特徴とするネットワーク接続方法。

2

【請求項７】　前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーは、

前記ユーザ認証のために授受する情報を暗号化し及び復号するための処理を実行することを特徴とする請求項６記載のネットワーク接続方法。

【請求項８】　ネットワークへの接続サービスをユーザ端末から受け付ける接続側サーバーと、ユーザに関する会員情報に基づいてユーザ認証を行う認証側サーバーと、を用いたネットワーク接続方法において、

ユーザ端末と認証側サーバーとの間で、ユーザＩＤ及びパスワードの授受を、前記接続側サーバーを経由して暗号を用いて行うために、

認証側サーバーが、一時的公開鍵Ｔ－Ｐｋを固有の秘密鍵Ｆ－Ｓｋで暗号化することによって第１の暗号データを作成するステップと、

認証側サーバーが、作成した前記第１の暗号データをユーザ端末に送信するステップと、

ユーザ端末が、送信された前記第１の暗号データから、前記固有の秘密鍵Ｆ－Ｓｋに対応する公開鍵Ｆ－Ｐｋを用いて前記一時的公開鍵Ｔ－Ｐｋを復号するステップと、

ユーザ端末が、復号した前記一時的公開鍵Ｔ－Ｐｋを用いて、ユーザＩＤ及びパスワードを暗号化することによって第２の暗号データを作成するステップと、

ユーザ端末が、作成した前記第２の暗号データを認証側サーバーに送信するステップと、

認証側サーバーが、送信された前記第２の暗号データから、前記一時的公開鍵Ｔ－Ｐｋに対応する一時的秘密鍵Ｔ－Ｓｋを用いてユーザＩＤ及びパスワードを復号するステップと、

を含むことを特徴とするネットワーク接続方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザ端末をインターネットなどの広域ネットワークに接続するためのネットワーク接続システム及びネットワーク接続方法の改良に関するもので、特に、接続サービスを提供する複数のサーバー間で、会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供するものである。

【０００２】

【従来の技術】近年、国際的な情報通信ネットワークとして、インターネットが急速に普及し、その重要性が増大しつつある。インターネットを利用する場合、一般のユーザは、インターネット接続業者（ＩＳＰ：インターネットサービスプロバイダ）と契約し、電話回線とモデ

ムを介してプロバイダのサーバーにログインし、サーバーを通じてインターネット上の情報にアクセスする。

【０００３】

【発明が解決しようとする課題】従来では、異なる複数のプロバイダのサーバー間で、会員情報及び回線接続設備を相互利用する手段は存在しなかったので、会員が接続できるのは契約先のプロバイダ（加入プロバイダ）のサーバーに限定されていた。このため、回線が混雑していて加入プロバイダのサーバーに接続できない場合でも、他のプロバイダのサーバーを介してインターネットに接続することはできなかった。この結果、加入プロバイダの回線混雑時に接続性が低下するという不都合が生じていた。また、電話回線使用料の観点から、ユーザもプロバイダも地理的に近い相手を契約対象として選ばざるを得なかった。このことは、ユーザによるプロバイダ選択の自由を狭めると共に、プロバイダによる新規会員募集の範囲も限定し、インターネットの普及を妨げていた。

【０００４】本発明は、上記のような従来技術の問題点を解決するために提案されたもので、その目的は、複数のサーバー間で会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供することである。また、本発明の他の目的は、会員情報を保有するサーバーと実際の接続を行うサーバーとの間で、接続に関する所定の情報を送受信することによって、双方で正副の同一内容の接続ログを記録し、接続ログの信頼性に優れたネットワーク接続システムを提供することである。

【０００５】また、本発明の他の目的は、ログイン時に接続側サーバーを経由するパスワードなどを暗号化することによって、セキュリティの優れたネットワーク接続システム及びネットワーク接続方法を提供することである。また、本発明の他の目的は、相互に所定の関係を有するサーバーの情報を、単一のメンバ登録用サーバーに登録し、メンバからの照会に応答することによって、信頼性とセキュリティに優れたネットワーク接続システムを提供することである。また、本発明の他の目的は、接続側と認証側のサーバー間で接続の継続を確認することによって、接続ログに記録される内容の信頼性が高いネットワーク接続システムを提供することである。

【０００６】

【課題を解決するための手段】上記の目的を達成するため、請求項１のネットワーク接続システムは、ネットワークへの接続回線設備を備えた複数のサーバーを有し、前記サーバーは、ユーザに関する会員情報を有する認証側サーバーと、前記認証側サーバーと所定の関係を有する接続側サーバーを含み、前記接続側サーバーは、ユーザから送信されるユーザＩＤ及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供する接続

手段を有し、前記認証側サーバーは、前記接続側サーバーから送信されるユーザＩＤ及びパスワードを前記会員情報と照合することによってユーザ認証を行うユーザ認証手段を有することを特徴とする。請求項６のネットワーク接続方法は、請求項１の発明を方法の観点から把握したものであって、ネットワークへの接続回線設備を備えた複数のサーバーを用い、前記サーバーは、ユーザに関する会員情報を有する認証側サーバーと、前記認証側サーバーと所定の関係を有する接続側サーバーを含むネットワーク接続システムにおいて、前記接続側サーバーは、ユーザから送信されるユーザＩＤ及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供し、前記認証側サーバーは、前記接続側サーバーから送信されるユーザＩＤ及びパスワードを前記会員情報と照合することによってユーザ認証を行うことを特徴とする。

【０００７】請求項１，６の発明では、ユーザーは、自己の会員情報を保有する認証側サーバーが混雑しているときや、認証側サーバーが地理的に遠い場合、他のサーバーである接続側サーバーにユーザＩＤとパスワードを送信することによってログイン要求を行う。ユーザが送信したユーザＩＤとパスワードは、接続側サーバーから認証側サーバーに転送され、認証側サーバーで会員情報と照合することによってユーザ認証が行われる。接続側サーバーでは、ユーザ認証の結果を受けてログイン処理が行われるので、ユーザはインターネット接続サービスを利用することができる。

【０００８】請求項２の発明は、請求項１記載のネットワーク接続システムにおいて、前記接続側サーバー及び認証側サーバーはそれぞれ、前記ネットワークへの接続の開始及び終了に関する所定の情報を送受信することによって、接続ログを記録する記録手段を有することを特徴とする。請求項２の発明では、接続側と認証側のサーバー間で情報を送受信することによって、双方同一内容のログを記録するので、ログの信頼性が向上する。

【０００９】請求項３の発明は、請求項２記載のネットワーク接続システムにおいて、前記接続側サーバーの前記記録手段及び前記認証側サーバーの前記記録手段は、前記接続の開始から終了に至る間、所定の間隔で所定の情報を送受信することによって前記接続が継続しているか否かを確認するように構成されたことを特徴とする。請求項３の発明では、接続開始から終了まで、接続側と認証側のサーバー間で接続が継続しているか否かの確認が所定の間隔で行われるので、接続ログに記録される内容の信頼性が向上する。

【００１０】請求項４の発明は、請求項１，２又は３記載のネットワーク接続システムにおいて、相互に所定の関係を有する複数のサーバーをメンバとして登録する登録手段と、任意のサーバーがメンバであるか否かの問い

合わせに応答するサーバー認証手段と、を有するメンバ登録用サーバーを備えたことを特徴とする。請求項４の発明では、複数のサーバーがグループのメンバとなって、会員情報及び接続回線設備を相互利用する場合、単一のメンバ登録用サーバーにメンバの情報が集中する。このため、サーバーごとにメンバの情報を保有して更新する必要がなくなり、更新ミスやメンバ情報の漏洩が生じにくく、優れたセキュリティが発揮される。

【００１１】請求項５の発明は、請求項１，２，３又は４記載のネットワーク接続システムにおいて、前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーが、前記ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段を有することを特徴とする。請求項７の発明は、請求項５の発明を方法の観点から把握したものであって、請求項６記載のネットワーク接続方法において、前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーは、前記ユーザ認証のために授受する情報を暗号化し及び復号するための処理を実行することを特徴とする。請求項５，７の発明では、パスワードなど、本来は認証側サーバー固有の情報は、暗号化された状態で接続側サーバーを通過する。このため、接続側サーバーや、パスワードが経由するインターネット上のサーバーによってパスワードなどの情報が盗取されることがない。

【００１２】請求項８の発明は、ネットワークへの接続サービスをユーザ端末から受け付ける接続側サーバーと、ユーザに関する会員情報に基づいてユーザ認証を行う認証側サーバーと、を用いたネットワーク接続方法において、ユーザ端末と認証側サーバーとの間で、ユーザＩＤ及びパスワードの授受を、前記接続側サーバーを経由して暗号を用いて行うために、認証側サーバーが、一時的公開鍵Ｔ－Ｐｋを固有の秘密鍵Ｆ－Ｓｋで暗号化することによって第１の暗号データを作成するステップと、認証側サーバーが、作成した前記第１の暗号データをユーザ端末に送信するステップと、ユーザ端末が、送信された前記第１の暗号データから、前記固有の秘密鍵Ｆ－Ｓｋに対応する公開鍵Ｆ－Ｐｋを用いて前記一時的公開鍵Ｔ－Ｐｋを復号するステップと、ユーザ端末が、復号した前記一時的公開鍵Ｔ－Ｐｋを用いて、ユーザＩＤ及びパスワードを暗号化することによって第２の暗号データを作成するステップと、ユーザ端末が、作成した前記第２の暗号データを認証側サーバーに送信するステップと、認証側サーバーが、送信された前記第２の暗号データから、前記一時的公開鍵Ｔ－Ｐｋに対応する一時的秘密鍵Ｔ－Ｓｋを用いてユーザＩＤ及びパスワードを復号するステップと、を含むことを特徴とする。

【００１３】請求項８の発明では、認証側サーバーが一時的公開鍵を発行し、ユーザ端末Ｔから接続側サーバー経由で認証側サーバーへ送信されるユーザＩＤ及びパスワードは、一時的公開鍵によって暗号化される。このため、ユーザＩＤ及びパスワードが接続側サーバーなどの第三者に盗取されることがなく、悪意ある接続側のプロバイダが、ユーザＩＤ及びパスワードを利用して接続の事実を偽装するなどの不正が回避できる。

【００１４】なお、ユーザＩＤ及びパスワードを暗号化する鍵として毎回変更される一時的公開鍵を用いるのは、暗号が経由する接続側サーバーが暗号自体をコピーして保存しておき、暗号を認証側サーバーに再送することによって実在しない接続を偽装し、不正な課金請求を起こすのを防止するためである。また、一時的公開鍵自体を暗号化するのは、端末Ｔ側で当該暗号を固有の公開鍵で復号することによって、当該一時的公開鍵が確かに認証側サーバーから送信されたものであることを確認できるようにするためである。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態（以下「実施形態」という）について、図面にしたがって具体的に説明する。

【００１６】（１）第１実施形態の構成

第１実施形態は、請求項１～５に対応するネットワーク接続システム（以下「本システム」という）及びこのネットワーク接続システム上で実行されるネットワーク接続方法（請求項６，７に対応）に関するものである。まず、図１は、本システムの概略的構成を示すブロック図である。

【００１７】この図に示すように、本システムは、ネットワークＮへの接続回線設備を備えた二つのサーバーＳ１，Ｓ２を有し、サーバーＳ１はユーザに関する会員情報Ｉを有する認証側サーバーになっており、サーバーＳ２は、認証側サーバーＳ１との提携関係（請求項１にいう「所定の関係」）を有する接続側サーバーになっている。認証側サーバーＳ１及び接続側サーバーＳ２はそれぞれ、通信サーバーＣを介してインターネットＮに接続され、ユーザ端末ＴはモデムＭを通じて通信サーバーＣにアクセスする。

【００１８】認証側サーバーＳ１及び接続側サーバーＳ２は、それぞれ、ホストプログラムＰ１，Ｐ２によって制御される。接続側サーバーＳ２及び認証側サーバーＳ１はそれぞれ、接続の事実を記録するための副ログＳ２２及び正ログＳ１２（請求項２にいう接続ログに相当するもの）を備え、副ログＳ２２及び正ログＳ１２には原則として同一の情報が記録される。

【００１９】また、本システムは、相互に提携関係を有するサーバーをメンバとして登録し、サーバーがメンバであるか否かの問い合わせに応答するサーバーであるセンタＳ３（請求項４にいうメンバ登録用サーバーに相当するもの）を備えている。

【００２０】図２は、本システムの認証側サーバーＳ１、接続側サーバーＳ２、ユーザ端末Ｔ及びセンタＳ３の具体的構成を示す機能ブロック図であり、この図にお

いて、図１に示したインターネットＮ、通信サーバーＣ及び各モデムＭは省略する。

【００２１】すなわち、接続側サーバーＳ２は、ユーザ端末Ｔから送信されるユーザＩＤ及びパスワードを用いて認証側サーバーＳ１にユーザ認証を求め、認証の結果に応じてユーザ端末Ｔにインターネットへの接続サービスを提供する接続手段Ｓ２１を有する。一方、認証側サーバーＳ１は、接続側サーバーＳ２から送信されるユーザＩＤ及びパスワードを会員情報Ｉと照合することによってユーザ認証を行うユーザ認証手段Ｓ１１を有する。また、接続側サーバーＳ２及び認証側サーバーＳ１はそれぞれ、接続開始及び接続終了に関する所定の情報を送受信することによって、副ログＳ２２及び正ログＳ１２を記録する記録手段Ｓ２３，Ｓ１３を有する。

【００２２】本システムを通してインターネットに接続するために、ユーザは、パーソナルコンピュータを所定の接続用プログラムで駆動して成るユーザ端末Ｔを用いる。このユーザ端末Ｔと認証側サーバーＳ１は、それぞれ、ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段Ｔ１及びＳ１４を有する。一方、接続用サーバーＳ２は、ユーザから送信された前記暗号を認証用サーバーＳ１に転送するように構成され、認証用サーバーＳ１は、転送された前記暗号からユーザＩＤ及びパスワードを復号する暗号管理手段Ｓ１４を有する。

【００２３】なお、接続側サーバーＳ２の記録手段Ｓ２２及び認証側サーバーＳ１の記録手段Ｓ１２は、所定の間隔で情報を交換することによってユーザによる接続が継続しているか否かを確認するように構成されている。

【００２４】また、センタＳ３は、相互に所定の関係を有するサーバーをメンバとしてメンバリストＳ３１に登録する登録手段Ｓ３２と、サーバーがメンバであるか否かの問い合わせに応答するサーバー認証手段Ｓ３３と、を有する。このセンタＳ３は、接続側サーバーＳ２と認証側サーバーＳ１との間で情報を交換するために必須なわけではないが、接続側サーバーＳ２及び認証側サーバーＳ１とは別の第三者的主体として、メンバの確認などを行うことによって安全性を高める効果があるので、設置されることが望ましい。各サーバーＳ１，Ｓ２，Ｓ３間の通信は、ＴＣＰ／ＩＰなどのインターネットプロトコル上で行われ、かつ、必要に応じて暗号化が施される。

【００２５】（２）第１実施形態の作用及び効果

上記のような構成を有する第１実施形態において、インターネットＮへの接続サービスは、次のような手順で行われる。なお、認証側サーバーＳ１及び接続側サーバーＳ２は、相互に提携関係を有するメンバとして、センタＳ３のメンバリストＳ３１にあらかじめ登録されているものとする。

【００２６】（２－１）事前準備

インターネット接続サービスを利用しようとするユーザは、所望のプロバイダを選択して接続サービスの契約を行う。この場合、本実施形態におけるユーザは、従来と異なり、地理的に遠いプロバイダであっても、自分にとって契約条件などが望ましいプロバイダを自由に選択して契約してよい。ユーザが契約したプロバイダ（加入プロバイダ）のサーバーには、ユーザの会員情報、特にユーザＩＤとパスワードが格納され、加入プロバイダ自身のサーバーが、本発明にいう認証側サーバーＳ１となる。ここでは、ユーザ端末Ｔのユーザに関し、ユーザＩＤ及びパスワードを含む会員情報Ｉが、認証側サーバーＳ１に登録されているものとする。

【００２７】加入プロバイダは、自己のサーバーへの接続用電話番号と共に、提携先プロバイダのサーバーへの接続用電話番号をユーザに知らせる。提携先プロバイダのサーバーが本発明にいう接続側サーバーＳ２である。提携は、プロバイダ相互間における１対１の関係には限定されず、何らかの組織に各プロバイダが加入することによって行うこともでき、この場合、センタＳ３のメンバリストＳ３１に登録されているプロバイダのサーバーが、相互に提携関係を有する正しい接続業者となる。

【００２８】（２－２）接続要求

図３は、第１実施形態における処理手順を示すフローチャートである。ユーザは、インターネット接続サービスを利用するときは、ユーザ端末Ｔと電話回線を用いて、サーバーに接続する。接続先となるサーバーは、通常は、加入プロバイダのサーバーＳ１である。しかし、加入プロバイダのサーバーＳ１の接続回線が混雑しているために電話がつながらない場合や、ユーザにとって加入プロバイダのサーバーＳ１が遠隔の場合、ユーザは、前記提携先プロバイダのサーバーＳ２に接続要求を行う（ステップ３０１）。

【００２９】なお、ユーザ端末Ｔは、専用の接続手順によって動作する。すなわち、接続要求にはユーザＩＤ及びパスワードを送信するが、加入プロバイダ以外のプロバイダに接続要求する場合は、ユーザ端末Ｔの暗号管理手段Ｔ１が、ユーザＩＤ及びパスワードを暗号化して接続側サーバーＳ２に送信する。なお、ユーザＩＤ及びパスワードを暗号化する場合でも、接続側サーバーＳ２で認証側サーバーＳ１を特定できるように、ユーザ端末Ｔは、暗号化されたユーザＩＤ及びパスワードに、認証側のプロバイダ又はサーバーを示す識別子を付加して接続側サーバーＳ２に送信する。また、識別子の付加に代えて、ユーザＩＤのうち、認証側サーバーＳ１を特定する表示の部分は暗号化せずに接続側サーバーＳ２に送信するようにしてもよい。例えば、ユーザＩＤの形式が"xxx@aaa.or.jp"の場合、"xxx"の部分は暗号化し、"@aaa.or.jp"の部分は暗号化せずに送信する。

【００３０】（２－３）サーバー認証

ユーザから接続要求を受けた接続側サーバーＳ２では、

接続手段Ｓ２１が接続要求を受け付ける。接続手段Ｓ２１は、接続要求に係るユーザＩＤの形式が他のサーバーのもの（例えば"xxx@aaa.or.jp"）である場合、当該他のサーバーＳ１(aaa.or.jp)がメンバであるか否かをセンタＳ３に問い合わせる（ステップ３０２）。問い合わせを受けたセンタＳ３では、サーバー認証手段Ｓ３３が、メンバリストＳ３１との照合によって、問い合わせに係る認証側サーバーＳ１がメンバであるか否かを確認し、問い合わせに回答する。

【００３１】（２－４）ユーザ認証

ユーザＩＤに係るサーバーＳ１がメンバであることが確認されると、接続側サーバーＳ２の接続手段Ｓ２１は、接続要求に係る認証側サーバーＳ１にユーザＩＤ及び暗号化されているパスワードを転送することによって、ユーザ認証（ユーザＩＤ及びパスワードが真正なものであるか否かを確認すること）を求める（ステップ３０３）。

【００３２】このとき、ユーザ認証を要求された認証側サーバーＳ１でも、認証要求を発行した接続側サーバーＳ２がメンバであるか否かをセンタＳ３に照会して確認する。問い合わせを受けたセンタＳ３は、メンバリストＳ３１と照合することによって、問い合わせに係る接続側サーバーＳ２がメンバであるか否かを確認し、問い合わせに回答する。問い合わせに係る接続側サーバーＳ２がメンバであることが確認されると、認証側サーバーＳ１の暗号管理手段Ｓ１４が、暗号からパスワードを復号する。

【００３３】そして、ユーザ認証手段Ｓ１１が、転送されてきたユーザＩＤ及び復号されたパスワードを会員情報Ｉと照合し、真正なユーザＩＤ及びパスワードであるか否かを確認することによってユーザ認証を行い、その結果を接続側サーバーＳ２に返信する。なお、サーバー認証やユーザ認証において、サーバーがメンバでなかったり、パスワードの不一致などで、否定的な結果となったときは、接続は当然に拒絶される。

【００３４】（２－５）接続開始と記録

返信されてきた認証結果が応諾（肯定的）ならば、接続側サーバーＳ２の接続手段Ｓ２１は、ユーザ端末Ｔとの間でＰＰＰ接続を開始する（ステップ３０４）と共に、記録手段Ｓ２３が認証側サーバーＳ１に接続開始通知を送信する（ステップ３０５）。認証側サーバーＳ１の記録手段Ｓ１３は、接続開始通知を受信すると、正ログＳ１２にユーザＩＤ及び開始時刻を記録する（ステップ３０６）と共に、接続開始受諾通知を接続側サーバーＳ２に送信する（ステップ３０７）。接続側サーバーＳ２の記録手段Ｓ２３は、接続開始受諾通知を受信すると、認証側サーバーＳ１の正ログＳ１２と同様に、ユーザＩＤ及び開始時刻を副ログＳ２２に記録する（ステップ３０８）。

【００３５】（２－６）接続の監視

その後、接続側サーバーＳ２における接続が終了し（ステップ３１０）、接続側サーバーＳ２から認証側サーバーＳ１に接続終了通知が送信されるまで、認証側サーバーＳ１は、接続が継続していることを一定間隔で接続側サーバーＳ２に確認することによって（ステップ３０９）、接続を監視する。

【００３６】（２－７）接続の終了

ユーザが所定の接続終了操作を行うと（ステップ３１０）、接続側サーバーＳ２の接続手段Ｓ２１がユーザ端末Ｔとの間でＰＰＰ接続を終了すると共に、記録手段Ｓ２３が認証側サーバーＳ１に接続終了通知を送信する（ステップ３１１）。認証側サーバーＳ１の記録手段Ｓ１３は、接続終了通知を受信すると、正ログＳ１２に接続終了の旨及び終了時刻を記録すると共に、接続終了確認通知を接続側サーバーＳ２に送信する。接続側サーバーＳ２の記録手段Ｓ２３は、接続終了確認通知を受信すると、認証側サーバーＳ１の正ログＳ１２と同様に、ユーザＩＤ及び終了時刻を副ログＳ２２に記録する。

【００３７】（２－８）課金の精算

認証側サーバーＳ１の正ログＳ１２及び接続側サーバーＳ２の副ログＳ２２は所定の期日に突合（照合）され、一致した接続に関して課金が精算される。

【００３８】（２－９）第１実施形態による効果

以上説明したように、第１実施形態によれば、ユーザーは、自己の会員情報を保有する認証側サーバーが混雑しているときや、認証側サーバーが地理的に遠い場合、他のサーバーである接続側サーバーにユーザＩＤとパスワードを送信することによって接続要求を行う。ユーザが送信したユーザＩＤとパスワードは、接続側サーバーから認証側サーバーに転送され、認証側サーバーで会員情報と照合することによってユーザ認証が行われる。接続側サーバーでは、ユーザ認証の結果を受けてユーザにインターネット接続サービスを提供する。

【００３９】これによって、混雑時でもネットワークへのつながりやすさ（接続可能性）が改善される。また、ユーザは遠隔のプロバイダとも契約できるので、プロバイダの会員募集の対象地域が拡大する。また、プロバイダは、独自に会員募集を行わず、接続側サーバーのみを提供することもできるので、プロバイダ経営が多様化する。第１実施形態によれば上記のような効果を通じて、インターネットの健全な普及が実現される。

【００４０】また、第１実施形態では、接続要求の際のパスワードなどの情報は、暗号化された状態でユーザから接続側サーバーを通過し認証側サーバーに到達する。このため、接続側サーバーのプロバイダによるパスワードなどの盗取が防止される。

【００４１】また、第１実施形態では、複数のサーバーがグループのメンバとなって、会員情報及び接続回線設備を相互利用する場合、単一のセンタにメンバの情報を蓄積しておくことができる。そして、接続側サーバー及

び認証側サーバーのいずれも、ユーザの接続要求に係る相手方がメンバか否かをセンタに問い合わせることによって確認できる。このため、メンバから脱退したプロバイダやメンバ以外のプロバイダなど、無権限な第三者が接続側サーバーのプロバイダになりすますことによって、接続サービスの課金請求を起こすことを回避できる。また、メンバーの情報は単一のセンタに蓄積される。このため、サーバーごとにメンバの情報を保有して更新する必要がなくなり、更新ミスやメンバ情報の漏洩が生じにくく、優れたセキュリティが発揮される。

【００４２】また、第１実施形態によれば、接続側と認証側のサーバー間で情報を送受信することによって、双方同一内容のログを記録するので、いずれかのサーバーによるログの偽造も防止され、ログの信頼性が向上する。

【００４３】また、第１実施形態によれば、接続開始から終了まで、接続側と認証側のサーバー間で接続が継続しているか否かの確認が所定の間隔で行われるので、接続ログに記録される内容の信頼性が向上する。

【００４４】（３）第２実施形態

前記第１実施形態においてもパスワード等を暗号化及び復号したが、パスワード等の暗号化に用いる鍵を毎回変更することによって、よりセキュリティ性を改善することができる。また、接続側サーバーＳ２と認証側サーバーＳ１との間で接続開始を通知したりログに記録する手順も第１実施形態に示したとおりである必要はない。第２実施形態は、第１実施形態と同様の構成を有するネットワーク接続システムにおいて、パスワード等の暗号化に用いる鍵を毎回変更することによって、よりセキュリティ性を改善した例であり（請求項８に対応）、また、接続側サーバーＳ２と認証側サーバーＳ１との間で接続開始を通知したりログに記録するなどの手順として、第１実施形態とは異なる手順を適用した例である。

【００４５】（３－１）ユーザ認証までの手順

図４は、第２実施形態における接続要求からユーザ認証までの処理手順を示すフローチャートである。すなわち、まず、ユーザ端末Ｔから接続側サーバーＳ２に接続要求があると（ステップ４０１）、接続側サーバーＳ２の接続手段Ｓ２１が、接続要求に係る認証側サーバーＳ１がメンバであることを、センタＳ３によるサーバー認証を求めて確認したうえ（ステップ４０２）、接続側サーバーＳ２から認証側サーバーＳ１へ新たな接続要求があったことを通知する（ステップ４０３）。

【００４６】接続要求の通知を受けた認証側サーバーＳ１のユーザ認証手段Ｓ１１でも、接続要求に係る接続側サーバーＳ２がメンバであることを、センタＳ３によるサーバー認証を求めて確認する（ステップ４０４）。なお、以下の説明で用いる暗号鍵は公開鍵暗号方式ＰＧＰを前提とし、

毎回変更される

一時的公開鍵Ｔ－Ｐｋ（暗号化用）

一時的秘密鍵Ｔ－Ｓｋ（復号用）

のペア及び固定された

固有の秘密鍵Ｆ－Ｓｋ（暗号化用）

固有の公開鍵Ｆ－Ｐｋ（復号用）

のペアを用いる。

【００４７】すなわち、接続側サーバーＳ２がメンバであることをサーバー認証で確認した認証側サーバーＳ１の暗号管理手段Ｓ１４は、一時的公開鍵Ｔ－Ｐｋを決定し、固有の秘密鍵Ｆ－Ｓｋで一時的公開鍵Ｔ－Ｐｋを暗号化することによって第１の暗号データを作成する（ステップ４０５）。一時的公開鍵Ｔ－Ｐｋは、端末Ｔから認証側サーバーＳ１へ、ユーザ認証のためのユーザＩＤ及びパスワードを暗号化して送信するためのものである。

【００４８】ここで、固有の秘密鍵Ｆ－Ｓｋは固定されたものであるが、一時的公開鍵Ｔ－Ｐｋは毎回変更される。認証側サーバーＳ１のユーザ認証手段Ｓ１１は、作成した前記第１の暗号データを、接続側サーバーＳ２を経由して端末Ｔに送信する（ステップ４０６）。端末Ｔには、固有の秘密鍵Ｆ－Ｓｋに対応する固有の公開鍵Ｆ－Ｐｋがあらかじめ与えられており、端末Ｔの暗号管理手段Ｔ１は、送信された前記第１の暗号データから、固有の公開鍵Ｆ－Ｐｋを用いて前記一時的公開鍵Ｔ－Ｐｋを復号する（ステップ４０７）。

【００４９】続いて、端末Ｔの暗号管理手段Ｔ１は、復号した前記一時的公開鍵Ｔ－Ｐｋを用いて、ユーザＩＤ及びパスワードを暗号化することによって第２の暗号データを作成し（ステップ４０８）、作成した前記第２の暗号データを、接続側サーバーＳ２を経由して認証側サーバーＳ１に送信する（ステップ４０９）。第２の暗号データを受信した認証側サーバーＳ１の暗号管理手段Ｓ１４は、送信された第２の暗号データから、前記一時的公開鍵Ｔ－Ｐｋに対応する一時的秘密鍵Ｔ－Ｓｋを用いてユーザＩＤ及びパスワードを復号する（ステップ４１０）。そして、認証側サーバーＳ１のユーザ認証手段Ｓ１１が、復号したユーザＩＤ及びパスワードを自己の会員情報Ｉと照合して真正なものであるか否かを確認することによってユーザ認証を行い（ステップ４１１）、その結果を接続側サーバーＳ２に通知する（ステップ４１２）。

【００５０】第２実施形態では、上記のように、認証側サーバーＳ１が一時的公開鍵Ｔ－Ｐｋを発行し、ユーザ端末Ｔから接続側サーバーＳ２経由で認証側サーバーＳ１へ送信されるユーザＩＤ及びパスワードは、一時的公開鍵Ｔ－Ｐｋによって暗号化される。このため、ユーザＩＤ及びパスワードが接続側サーバーＳ２などの第三者に盗取されることがなく、悪意ある接続側のプロバイダが、ユーザＩＤ及びパスワードを利用して接続の事実を偽装するなどの不正が回避できる。

【００５１】なお、ユーザＩＤ及びパスワードを暗号化する鍵として毎回変更される一時的公開鍵Ｔ－Ｐｋを用いるのは、暗号が経由する接続側サーバーＳ２が暗号自体をコピーして保存しておき、暗号を認証側サーバーＳ１に再送することによって実在しない接続を偽装し、不正な課金請求を起こすのを防止するためである。また、一時的公開鍵Ｔ－Ｐｋ自体を暗号化するのは、端末Ｔ側で当該暗号を固有の公開鍵Ｆ－Ｐｋで復号することによって、当該一時的公開鍵Ｔ－Ｐｋが確かに認証側サーバーＳ１から送信されたものであることを確認できるようにするためである。

【００５２】（３－２）ユーザ認証以降の手順

図５は、第２実施形態において、ユーザ認証以降の手順を示すフローチャートである。すなわち、正しいユーザＩＤ及びパスワードによってユーザ認証が無事に終了すると、認証側サーバーＳ１の記録手段Ｓ１３は、センタＳ３及び接続側サーバーＳ２に、接続許諾通知と接続の開始時刻を通知するとともに、その旨と開始時刻を正ログＳ１２に記録する（ステップ５０１）。接続側サーバーＳ２では、この通知を受け、接続手段Ｓ２１がユーザ端末Ｔとの間でＰＰＰ接続を開始すると同時に、記録手段Ｓ２３が接続開始時刻を副ログＳ２２に記録する（ステップ５０２）。なお、センタＳ３及び接続側サーバーＳ２は、接続許諾通知を受信した場合、受信確認を認証側サーバーＳ１へ送信する（ステップ５０３）。

【００５３】接続開始後は、接続側サーバーＳ２及び認証側サーバーＳ１は、接続終了まで、それぞれ一定間隔で他方に対して接続が継続していることを確認する。すなわち、接続側サーバーＳ２の記録手段Ｓ２３は、ユーザによる接続終了操作が行われたり回線切断による自動ログアウトが発生するまで、認証側サーバーＳ１の記録手段Ｓ１３に対して一定間隔で、接続の継続を表すデータを送信する。そして、接続側サーバーＳ２の記録手段Ｓ２３は、この送信に対して確認のための返信を認証側サーバーＳ１の記録手段Ｓ１３から受けることによって、認証側サーバーＳ１が接続の継続を認識していることを確認する（ステップ５０５）。

【００５４】一方、認証側サーバーＳ１の記録手段Ｓ１３は、接続側サーバーＳ２から接続終了の通知を受け取るまで、接続側サーバーＳ２の接続手段Ｓ２１に対して一定間隔で、接続の継続を問い合わせるデータを送信する。そして、認証側サーバーＳ１の記録手段Ｓ１３は、この送信に対する返信を接続側サーバーＳ２の接続手段Ｓ２１から受信することによって、接続側サーバーＳ２における接続が継続していることを確認する（ステップ５０６）。

【００５５】接続側サーバーＳ２の記録手段Ｓ２３は、ユーザの端末Ｔから接続終了を表す信号を受け取った場合（ステップ５０４）、認証側サーバーＳ１及びセンタＳ３に接続終了通知と接続終了時刻を送信する（ステップ５０７）。認証側サーバーＳ１の記録手段Ｓ１３は、接続終了通知及び接続終了時刻を受信した場合、正ログＳ１２に接続終了の旨及び接続終了時刻を記録すると共に（ステップ５０８）、接続側サーバーＳ２及びセンタＳ３へ接続終了確認通知を送信する（ステップ５０９）。この接続終了確認通知を受信した接続側サーバーＳ２の記録手段Ｓ２３は、副ログＳ２２に接続終了の旨及び接続終了時刻を記録する。

【００５６】なお、接続の開始や終了は、接続側サーバーＳ２及び認証側サーバーＳ１からの通知を受けて、センタＳ３でも所定のログ（図示せず）に記録される。そして、認証側サーバーＳ１及び接続側サーバーＳ２の正ログＳ１２及び副ログＳ２２は、所定の期日にセンタＳ３へ送られ、センタＳ３のログを含む計３つのログが相互に突合され、一致しているデータが課金請求などの処理へ回される。

【００５７】第２実施形態では、上記のように、接続開始通知や接続開始時刻など接続に関する情報がセンタＳ３にも送信され、センタＳ３でも正ログＳ１２や副ログＳ１３と同様の記録が行われるので、ログの正確性と信頼性が一層向上する。

【００５８】また、第２実施形態では、接続継続の確認は、認証側から接続側及び接続側から認証側へという双方向で行われる。これによって、まず、接続側サーバーＳ２がダウンしたり、又は障害のために認証側に終了通知を送信できない場合も、認証側からの確認によって接続の終了が判明するので、認証側サーバーＳ１は、接続の終了を正しく接続ログに記録することができる。また、認証側サーバーＳ１がダウンしたり、又は障害のために接続側からの終了通知を認識できない場合も、接続側サーバーＳ２は確認によってそれらの事態を把握し、例外処理を起動するなど必要な処理を行うことができる。

【００５９】（４）他の実施形態

なお、本発明は上記実施の形態に限定されるものではないので、次に例示するような他の実施の形態をも包含するものである。例えば、接続側サーバーと認証側サーバーという種別はユーザとの関係で定まる相対的なもので、具体例を挙げれば、図２の接続側サーバーＳ２が独自に会員と会員情報を持っていても差しつかえない。すなわち、認証側サーバーは、接続要求に係るユーザの会員情報を保有しているサーバーを意味し、サーバーＳ２のプロバイダと契約しているユーザがサーバーＳ１に接続要求する場合は、ユーザにとっては、前記各実施形態とは逆に、サーバーＳ１が接続側サーバーとなり、サーバーＳ２が認証側サーバーとなる。

【００６０】また、メンバ登録用サーバーであるセンタＳ３は必ずしも設ける必要はなく、認証側サーバー及びユーザ端末の暗号管理手段を設けずに本発明を実施することも技術的には可能である。また、本発明は、インタ

15　　16

ーネットへの接続のみならず、他の広域ネットワークへの接続にも適用することができる。

【００６１】

【発明の効果】以上説明したように、本発明によれば、複数のサーバー間で会員情報及び接続回線設備を相互利用できるので、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態の概略的構成を示すブロック図

【図２】本発明の第１実施形態の要部の構成を示す機能ブロック図

【図３】本発明の第１実施形態における処理手順を示すフローチャート

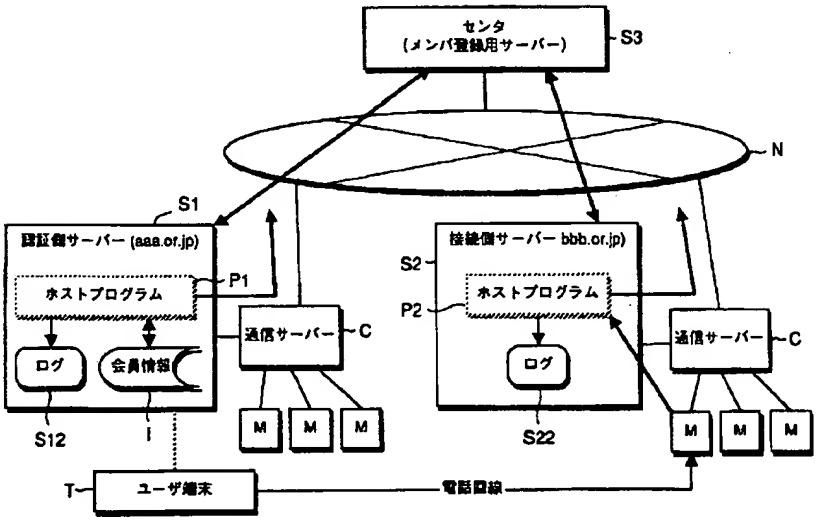
【図４】本発明の第２実施形態におけるユーザ認証までの処理手順を示すフローチャート

【図５】本発明の第１実施形態におけるユーザ認証以降の処理手順を示すフローチャート

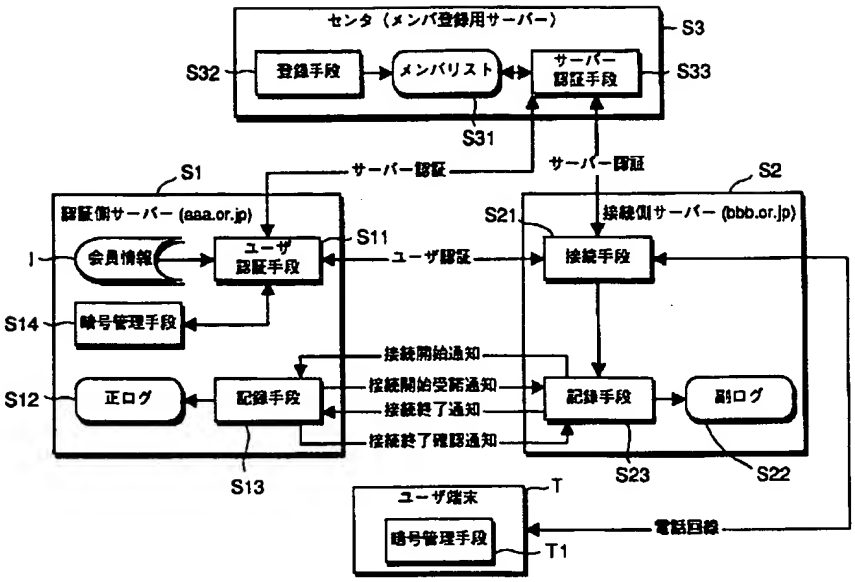
【符号の説明】

Ｓ１…認証側サーバー
Ｓ１１…ユーザ認証手段
Ｓ１２…正ログ
Ｓ１３…記録手段
Ｓ１４…暗号管理手段
Ｓ２…接続側サーバー
Ｓ２１…接続手段
Ｓ２２…副ログ
Ｓ２３…記録手段
Ｓ３…センタ（メンバ登録用サーバー）
Ｓ３１…メンバリスト
Ｓ３２…登録手段
Ｓ３３…サーバー認証手段
Ｃ…コミュニケーションサーバー
Ｉ…会員情報
Ｍ…モデム
Ｎ…インターネット
Ｐ１，Ｐ２…ホストプログラム
ＳＴＥＰ…手順の各ステップ
Ｔ…ユーザ端末
Ｔ１…暗号管理手段

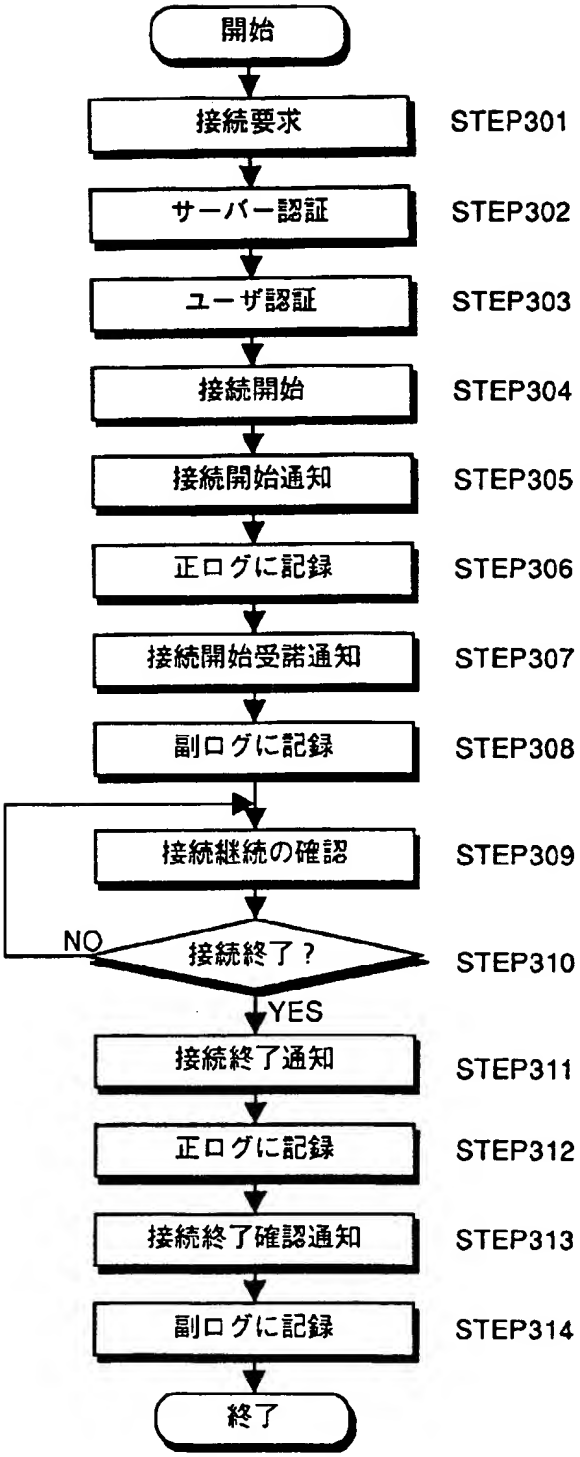
【図１】



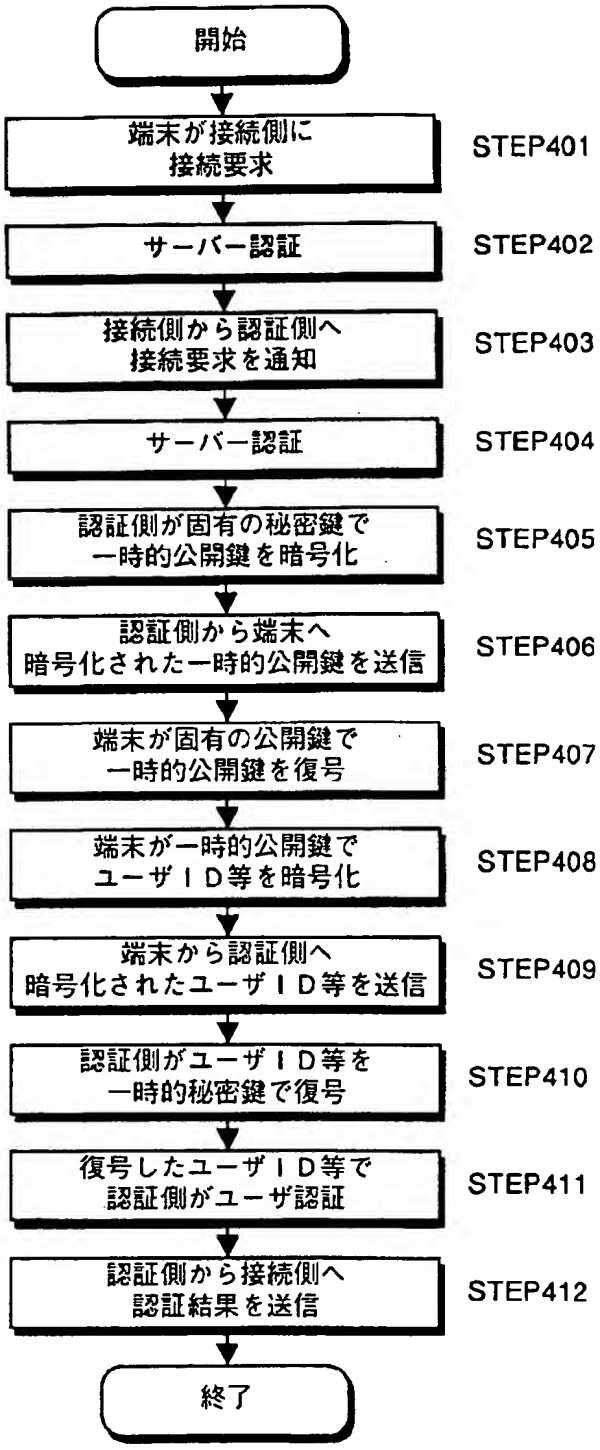
【図２】


センタ（メンバ登録用サーバー）
S3
S32
登録手段
メンバリスト
サーバー認証手段
S33
S31
サーバー認証
サーバー認証
S1
S2
認証側サーバー (aaa.or.jp)
接続側サーバー (bbb.or.jp)
S21
S11
会員情報
ユーザ認証手段
ユーザ認証
接続手段
S14
暗号管理手段
接続開始通知
S12
正ログ
記録手段
接続開始受諾通知
接続終了通知
記録手段
副ログ
接続終了確認通知
S13
S23
S22
T
ユーザ端末
電話回線
暗号管理手段
T1

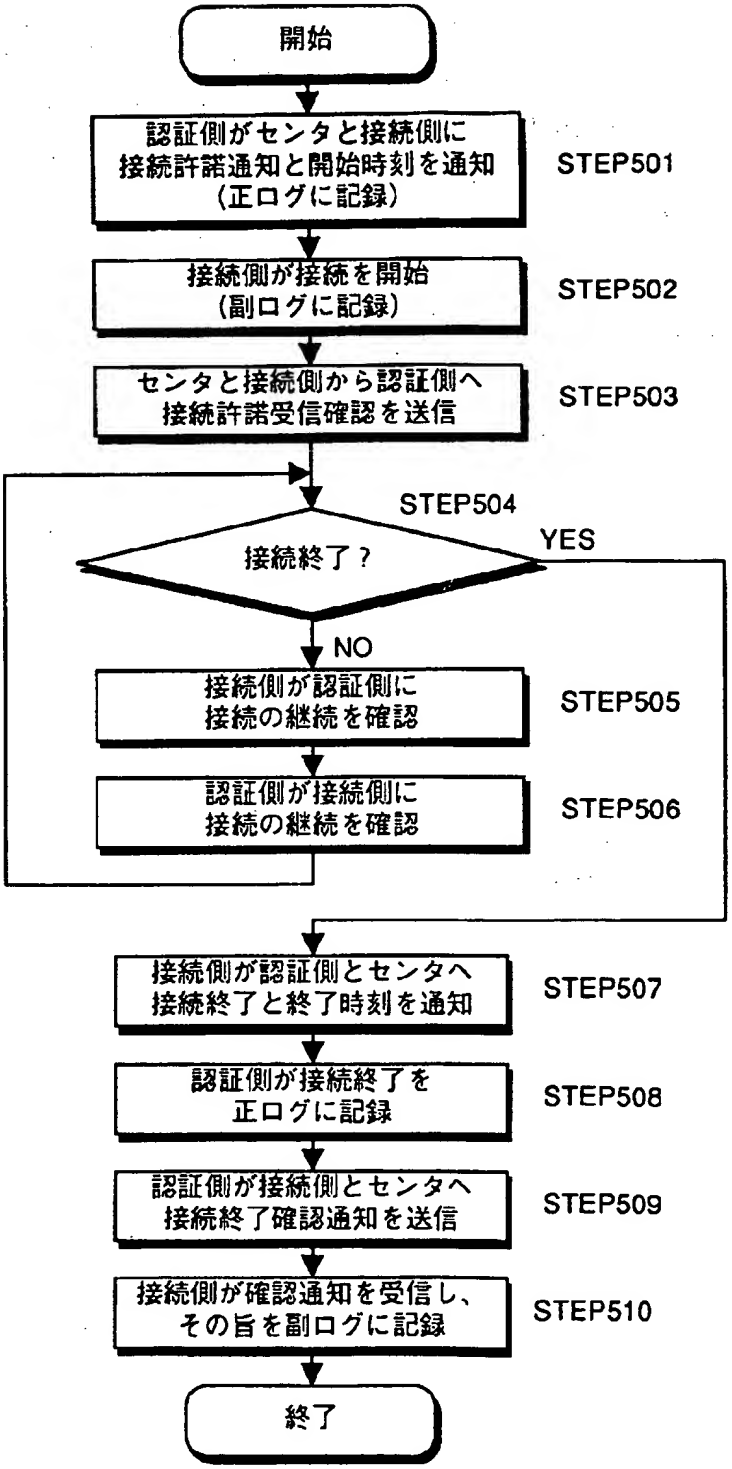
【図３】


開始
接続要求
STEP301
サーバー認証
STEP302
ユーザ認証
STEP303
接続開始
STEP304
接続開始通知
STEP305
正ログに記録
STEP306
接続開始受諾通知
STEP307
副ログに記録
STEP308
接続継続の確認
STEP309
NO
接続終了？
STEP310
YES
接続終了通知
STEP311
正ログに記録
STEP312
接続終了確認通知
STEP313
副ログに記録
STEP314
終了

【図４】


開始
端末が接続側に接続要求
STEP401
サーバー認証
STEP402
接続側から認証側へ接続要求を通知
STEP403
サーバー認証
STEP404
認証側が固有の秘密鍵で一時的公開鍵を暗号化
STEP405
認証側から端末へ暗号化された一時的公開鍵を送信
STEP406
端末が固有の公開鍵で一時的公開鍵を復号
STEP407
端末が一時的公開鍵でユーザＩＤ等を暗号化
STEP408
端末から認証側へ暗号化されたユーザＩＤ等を送信
STEP409
認証側がユーザＩＤ等を一時的秘密鍵で復号
STEP410
復号したユーザＩＤ等で認証側がユーザ認証
STEP411
認証側から接続側へ認証結果を送信
STEP412
終了

【図５】


開始
認証側がセンタと接続側に
接続許諾通知と開始時刻を通知
(正ログに記録)
STEP501
接続側が接続を開始
(副ログに記録)
STEP502
センタと接続側から認証側へ
接続許諾受信確認を送信
STEP503
STEP504
接続終了？
YES
NO
接続側が認証側に
接続の継続を確認
STEP505
認証側が接続側に
接続の継続を確認
STEP506
接続側が認証側とセンタへ
接続終了と終了時刻を通知
STEP507
認証側が接続終了を
正ログに記録
STEP508
認証側が接続側とセンタへ
接続終了確認通知を送信
STEP509
接続側が確認通知を受信し、
その旨を副ログに記録
STEP510
終了

フロントページの続き

(51)Int.Cl.[6]	識別記号	FI
		673　A

(72)発明者　山本　厳淳
北海道札幌市中央区南２条西７丁目６－２
日宝南２条ビル５階　株式会社アド・ホック内